SISTEMAS OPERATIVOS
Seguridad

SUAYED
Ricardo Mancilla Guzmán
410110724
ricardomancillag@hotmail.com
rickman@comunidad.unam.mx

Resumen

El principal programa de un sistema es un sistema operativo, que es el responsable del control de todos los recursos de la computadora y proporciona la base sobre el cual pueden escribirse los programas de aplicación.

Introducción

Es un conjunto de programa que crean la interfaz del hardware con el usuario y que tiene dos funciones primordiales:

Gestionar el hardware, se refiere a hecho de administrar una forma más eficiente los recursos de la máquina.

Facilitar el trabajo al usuario ya que permite una comunicación con los dispositivos de la máquina.

Título Principal

Descripción:
El entorno de la seguridad, aspectos básicos de la criptografía, cómo se lleva a cabo la autenticación de usuarios y algunos mecanismos de protección que los sistemas operativos implementan.

Los sistemas de archivos a menudo contienen información que es muy valiosa para sus usuarios. Por tanto, la protección de esta información contra el uso no autorizado es una función importante de todos los sistemas de archivos. En las siguientes secciones examinaremos diversos problemas relacionados con la seguridad y la protección. Estas cuestiones se aplican tanto a los sistemas tiempo compartido como a las redes de computadoras personales conectadas a servidores compartidos a través de redes de área local.

La verificación de autenticidad es otro problema en los sistemas de mensajes: ¿cómo puede el cliente saber que se está comunicando con el verdadero servidor de archivos, y no con un impostor?

En el otro extremo del espectro, hay aspectos de diseño que son importantes cuando el emisor y el receptor están en la misma máquina. Uno de éstos es el rendimiento. El copiado de mensajes de un proceso a otro siempre es más lento que efectuar una operación de semáforo o entrar en un monitor. Se ha trabajado mucho tratando de hacer eficiente la transferencia de mensajes. Cheriton (1984), por ejemplo, ha sugerido limitar el tamaño de los mensajes a lo que cabe en los registros de la máquina, y efectuar luego la transferencia de mensajes usando los registros.

Muchos esquemas de protección se basan en el supuesto de que el sistema conoce la identidad de cada usuario. El problema de identificar los usuarios cuando inician una sesión se denomina verificación de autenticidad de usuarios. La mayor parte de los métodos de verificación de autenticidad se basan en identificar algo que el usuario conoce, tiene o es.

La forma de verificación de autenticidad más ampliamente utilizada es pedir al usuario que teclee una contraseña. La protección mediante contraseña es fácil de entender y de implementar. En UNIX el esquema funciona como sigue. El programa de inicio de sesión pide al usuario que teclee su

nombre y contraseña. De inmediato, la contraseña se cifra. Luego, el programa de inicio de sesión lee el archivo de contraseñas, que es una serie de líneas ASCII, una por usuario, hasta encontrar la que contiene el nombre de inicio de sesión del usuario. Si la contraseña (cifrada) contenida en esta línea concuerda con la contraseña cifrada que se acaba de calcular, se permite el inicio de la sesión; de lo contrario, se rechaza.
La verificación de autenticidad de las contraseñas es fácil de vencer. Es frecuente leer acerca de grupos de estudiantes de preparatoria, o incluso de secundaria, que, con la ayuda de sus computadoras caseras, se introducen en algún sistema de secreto máximo, propiedad de una corporación gigantesca o una dependencia del gobierno. Prácticamente en todos los casos la intrusión se efectúa adivinando una combinación de nombre de usuario y contraseña.

Los términos "seguridad" y "protección" con frecuencia se usan indistintamente. No obstante, suele ser útil hacer una distinción entre los problemas generales que debemos resolver para asegurar que los archivos no sean leídos ni modificados por personas no autorizadas, lo que incluye cuestiones técnicas, gerenciales, legales y políticas, por un lado, y los mecanismos específicos del sistema operativo que proporcionan seguridad, por el otro. A fin de evitar confusiones, usaremos el término seguridad para referimos al problema global, y el término mecanismos de protección para referimos a los mecanismos específicos del sistema operativo que sirven para salvaguardar la información en la computadora. Sin embargo, la frontera entre las dos cosas no está bien definida. Primero examinaremos la seguridad; más adelante nos ocuparemos de la protección.
La seguridad tiene muchas facetas. Dos de las más importantes son la pérdida de datos y los intrusos. Algunas de las causas comunes de la pérdida de datos son:
1. Actos divinos: incendios, inundaciones, terremotos, guerras, motines o ratas que mordisquean cintas o disquetes.
2. Errores de hardware o software: fallas de CPU, discos o cintas ilegibles, errores de telecomunicación, errores en programas.
3. Errores humanos: captura incorrecta de datos, montar la cinta o disco equivocado, SEC. 5.4 SEGURIDAD 435
ejecutar un programa indebido, perder un disco o una cinta, o alguna otra equivocación.
La mayor parte de estos problemas puede superarse manteniendo respaldos adecuados, de preferencia lejos de los datos originales.
Un problema más interesante es qué hacer respecto a los intrusos. Hay dos clases de estos especímenes. Los intrusos pasivos sólo desean leer archivos que no están autorizados para leer. Los intrusos activos tienen peores intenciones: quieren efectuar cambios no autorizados a los datos. Al diseñar un sistema de modo que sea seguro frente a los intrusos, es importante tener presente la clase de intruso contra la que se está tratando de proteger el sistema. He aquí algunas categorías comunes:
1. Curioseo casual por parte de usuarios no técnicos. Muchas personas tienen en su escritorio terminales conectadas a sistemas de tiempo compartido o computadoras personales conectadas a redes y, al ser la naturaleza humana como es, algunas de ellas leerán el correo electrónico y otros archivos de otras personas si no se les ponen barreras. En la mayor parte de los sistemas UNIX, por ejemplo, todos los archivos están abiertos al público por omisión.
2. Intromisión por parte de gente de adentro. Los estudiantes, programadores de sistemas, operadores y demás personal técnico con frecuencia consideran como un reto personal violar la seguridad del sistema de computadora local. Es común que estas personas estén altamente capacitadas y dispuestas a dedicar una cantidad sustancial de tiempo a esta labor.
3. Intento decidido por hacer dinero. Algunos programadores bancarios han intentado introducirse en un sistema bancario para robar. Los ardides han variado desde modificar el software para truncar en lugar de redondear los intereses, guardándose la fracción de centavo para sí, hasta extraer fondos de cuentas que no se han usado en varios años, hasta chantaje ("Páguenme o destruiré todos los registros del banco").
4. Espionaje comercial o militar. Por espionaje se entiende el intento serio y bien financiado, por parte de un competidor o un país extranjero, por robar programas, secretos comerciales, patentes, tecnología, diseños de circuitos, planes de marketing, etc. En muchos casos este intento implica intervención de líneas o incluso erigir antenas dirigidas hacia la computadora a fin de captar su radiación electromagnética.

https://archive.org/details/8891410110724.4.9.1